amazon.com

June 12, 2018

The Honorable Charles Grassley
Chairman, Committee on the Judiciary
United States Senate
224 Dirksen Senate Office Building
Washington, D.C., 20510

Dear Chairman Grassley,

Thank you for your May 29, 2018 letter regarding Amazon.com's policies and procedures with respect to sharing customer data with third party developers, and related matters.

We disclose in our privacy notice the types of data we collect and the limited circumstances in which we share customer data with third parties. We also strive to design our products and services so that it is easy for customers to understand when their data is being collected or shared. Where appropriate, we also provide conspicuous messaging or other signals about data collection and sharing as part of the user experience.

We are not in the business of selling our customers' personal data. We sell products and services to our customers, and we remain obsessed with earning and keeping customer trust. Our customers know that their personal information is safe with us, and we know that we must get privacy right in order to meet our customers' high expectations. We use our customer data to innovate and improve the customer experience, and we focus on privacy at all stages of product development through privacy-by-design principles and through robust controls and practices.

The answers to your specific questions are as follows:

1. **What are your current policies and procedures with respect to the sharing of data with third party developers, including how you notify users of such sharing and/or request theirconsent?**
   a. **How have these policies and procedures evolved/changed since 2010?**
   b. **Do you intend to make any changes in light of recent events?**

We design our products and services to limit the amount of personally identifiable information that may be shared, and to share that information in a way that's transparent to our customers. We do not share a customer's personally identifiable information with developers through these products and services without the customer's agreement. We take the privacy and security of our customers' data seriously, and we regularly review our privacy practices and related customer messaging and revise them as appropriate.

For example, when a customer with an Echo device interacts with an Alexa "skill" (Alexa's equivalent of an app) provided by a third-party developer, we do not share the customer's identity with the skill developer. Only when a customer chooses to share their identity with a developer – e.g., if a customer takes steps to link their Amazon account to their Uber account so they can request a ride through Alexa – is the developer able to associate usage of the developer's skill with a customer's name. We share with the developer the content of the customer's request to the skill so the skill can respond accordingly, but we share only that personally identifiable information to which the customer has granted the developer access.

We use a permission framework similar to the one used by mobile devices, which requires customers to grant access to share certain data with developers – e.g., Uber could request access to the address the customer has set for their Echo device so they can send a ride to that location, and we would only share that address with

Uber after the customer granted access. As a result, customers are involved anytime we share their personally identifiable information with a skill developer. Customers can also change these permissions anytime from their Alexa app.

Similarly, when a customer downloads an app from our Appstore, we do not share the customer's identity with the app developer. Customers may choose to provide information directly to the app developer from within the app, such as by creating a Spotify account and providing their account information in the Spotify app. In the rare cases where we need to share customers' information directly with app developers, we are transparent and ask customers' permission. For example, for certain types of subscription purchases, we share customers' order information with the developer for purposes of fulfilling the order, and we give customers the option to share their name, billing address, and email address with the developer for marketing purposes. We inform customers of this option on the purchase screen before they make their purchase, and give customers the ability to check or uncheck the option to share this information for marketing purposes. Customers can also adjust this option anytime from their Appstore settings.

Our "Login with Amazon" service similarly illustrates our approach. For example, Login with Amazon gives customers the choice to securely log in to a third party site with their Amazon account, rather than create a new account log in with the third party site. Authentication is handled by Amazon on Amazon servers, reducing the amount of personally identifiable information customers must give to third party developers to use their sites.

As part of this process, customers can agree to share basic profile information or interests with the third party site, which is data customers normally share when separately creating profiles directly on those sites. The customer is shown the types of information the third party would like to see and allowed to select what information to share. Importantly, the customer can change permissions at any time. A customer can visit the Manage Login with Amazon page in "Your Account" settings on Amazon.com to see a list of the third parties the customer is sharing information with (including the specific types of information being shared), and make changes if desired.

For example, a customer who is shopping online at Atomtickets.com can share her email address through Login with Amazon, skipping the account creation process and avoiding the hassle of remembering additional user names or passwords. The customer can log in to her Amazon account to see the email address she is sharing with Atom and can click the "Remove" button to stop sharing it, at any time.

As the examples above highlight, a customer's personally identifiable information will not be shared with developers unless the customer shares it with a developer directly, or directs Amazon to do so. We don't, for example, have developer-facing application programming interfaces (APIs) that provide customers' personally identifiable information to developers independent of the customer interacting with that developer and electing to share their personally identifiable information with the developer.

2. How do you ensure that user data shared with third party developers is not improperly transferred or used?

As discussed above, customers are in control of the personally identifiable information they share with third party developers through our programs. However, third party developers are also subject to separate and additional agreements with us with respect to the customer data they collect.

Continuing with the examples described above, whenever there is a possibility we may enable a customer to share personally identifiable information with third party app or skill developers, our agreement with the developer requires them to (a) provide us with a privacy notice, which we post on the detail page for the skill in our skill store or app in our Appstore, (b) obtain appropriate consents from customers for the collection, use, and transfer of the information, (c) use the information only for the purposes permitted by the customer, and (d) ensure the information is collected, used, and transferred in accordance with the developer's privacy notice and applicable law.

As just one example, our Login with Amazon Service Agreement states that the developer must obtain express consent from the customer to keep any data it received through Login with Amazon (e.g., to maintain a customer's preferences when interacting directly with that third-party site). If consent is not sought from the customer, the developer must delete the information it has.

3. Do you limit the ability of third party developers to collect data beyond the scope of their application? If so, how do you ensure that third party developer agreements are limited in scope?

Our programs provide access to a customer's personally identifiable information only when the customer has granted the third party developer access to that information.

First and foremost, we design our programs to make it apparent to customers when their personally identifiable information is being provided to a third party developer, and we provide users with access to the developer's privacy notice so they may review the developer's privacy practices prior to sharing their information. We also make it simple and easy for customers to change their decision to share information later.

In addition to the agreement terms described above, we also have policies that require developers to use a customer's personally identifiable information only for the purposes the customer has permitted.[1]

4. What remedies do you have against a third party developer who exceeds the scope of their access?

If a third party developer violates their agreement with us, we have a number of remedies we can take, and we select the appropriate one based on the violation. We can terminate our agreement with the developer, as well as the developer's account and the developer's access to any APIs and other services the developer uses. For our skill and app programs, we can withdraw the developer's apps and skills from distribution through our stores. We also have standard contractual remedies (e.g., liability for breach) we can pursue.

5. Do you have protocols built into your third party developer platform to monitor data usage or access?

Our programs provide access to a customer's personally identifiable information only when the customer has granted the third party developer access to that information. For example, one way this is accomplished technically is by requiring the developer to present a valid access token to access the endpoints that provide the information or requiring the developer to verify the status of their access to information through API calls.

[1] For example, see https://developer.amazon.com/docs/custom-skills/permissions-configuration.html *("Request particular permissions in your skill only when these permissions are required to support the features and services provided by your skill. You must use any personal information you request only as permitted by the user and in accordance with your privacy notice and applicable law.")*

6. **What audit procedures do you have to ensure compliance with third party developer agreements?**
    a. **How often have these audits been carried out?**
    b. **How compliant have third party developers been?**

Amazon customers have access to more than 40,000 skills and 700,000 apps, and more than 24,000 live sites and apps where Login with Amazon is available. The vast majority of skills and apps do not ask customers for personally identifiable information. Skills and apps undergo testing against our security and technical requirements prior to publication. Login with Amazon has a registration process that requires third parties to list all information needed for the integration and why, and we will not approve integrations that request access to information beyond what that third party needs to provide the customer with the service. Additionally, if, through our own testing or customer feedback (e.g., we have a tool that detects a drop in app ratings, triggering an investigation), we have concerns about a developer’s privacy practices, we raise them to the developer and/or withdraw the skill or app from the store, depending on the concern. We monitor customer service contacts and are responsive to any customer concerns.

7. **Have third party developers breached your terms/agreements in the past, and what remedies have you taken?**

We have exercised the rights described above (e.g., terminated the developer’s agreement, account, and access to Amazon services the developer uses, and withdrawn their skills and apps from our store) when developers have failed to comply with the terms of our agreements or policies, such as by failing to comply with our policies for acceptable content within apps and skills.

8. **What are your current policies and procedures with respect to notifying users of a data breach?**
    a. **How have these policies and procedures evolved/changed since 2010?**
    b. **Do you intend to make any changes in light of recent events?**

We will notify customers of a breach involving their data as soon as reasonably possible after investigating the breach. If a breach occurs, we investigate the breach, determine the impacted data points, identify the impacted customers, identify the cause of the breach, and remediate the breach. Our policy regarding notification of customers is focused on what is the best thing to do for customers. We regularly review our policies regarding breach assessment and notification, and make changes as appropriate, including those required by law.

9. **What are your current policies and procedures with respect to notifying users of an improper transfer of their data?**
    a. **How have these policies and procedures evolved/changed since 2010?**
    b. **Do you intend to make any changes in light of recent events?**

See answer to question eight.

10. **Do you restrict the ability of third party developers to access data for a political purpose?**

Developers only receive customer data in connection with a service the developer provides to the customer, and we require the developer to use that data only for the purposes permitted by the customer. By interacting with a political campaign’s skill or app, a customer could choose to allow a developer to use their data for a political purpose.

11. What engagement do you have with political campaigns and do you have policies and procedures governing these engagements?

- **a. How have these policies and procedures evolved/changed since 2010?**
- **b. Do you intend to make any changes in light of recent events?**

We allow political campaigns to publish skills on Alexa or apps in our Appstore, and they must comply with our standard content policies. We do not provide tools to allow political campaigns to specifically target or influence our customers outside the developer's skill or app experience. Customers must interact with a skill, or download an app from the Amazon Appstore, in order to see the developer's skill or app content. We also do not sell political advertising.

12. How do you monitor the ability of foreign entities to access user data? What restrictions are in place to limit such access?

We take the security and privacy of our customers' information seriously. We routinely assess threats and vulnerabilities to the security of our systems and services. This applies to all bad actors, including foreign entities.

Our agreements with developers restrict entities that are subject to sanctions or otherwise designated on any list of prohibited or restricted parties maintained by the United States government or other applicable government authority from using our services. Additionally, if, through our own testing or customer feedback, we have concerns about a developer's practices, we raise them to the developer and/or withdraw the skill or app from the store. We also monitor customer service contacts and are responsive to any customer concerns.

13. How do you monitor the ability of foreign entities to influence and interfere with U.S. elections?

This question appears to be directed to social media companies and news services. Amazon customers may interact with a skill, or download an app from the Amazon Appstore in order to see the developer's skill or app content. Our standard content policies prohibit illegal activity, and Amazon does not otherwise monitor or control customer interaction with third party content.

14. Are you aware of any foreign entities seeking to influence or interfere with U.S. elections through your platforms?

No.

Thank you again for your interest in these issues, and our approach to policies and procedures with respect to sharing customer data with third party developers, and related matters.

Sincerely,

Brian Huseman
Vice President, Public Policy

CC: The Honorable Diane Feinstein
Ranking Member, Committee on the Judiciary
United States Senate